

Note sur la protection des données à caractère personnel et données de santé

Préambule

Cette note est destinée à l'information des professionnels de santé et des professionnels médico-sociaux qui utilisent le Webmail Medimail, mais également aux Usagers qui souhaiteraient être informés des modalités de traitement de leurs données à caractère personnel par la solution de messagerie sécurisée de santé **Medimail**.

L'Utilisation de la messagerie Sécurisée de Santé **Medimail** nécessite la collecte et le traitement de données à caractère personnel au sens :

- Du Règlement UE 2016/679 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données du 27 avril 2016 (« RGPD »)
- De la loi 78-17 du 6 janvier 1978 modifiée relative à l'Informatique, aux Fichiers et aux Libertés (« Loi I&L »)
- De l'article L.1111-8 du Code de la santé publique

Le RGPD, la Loi I&L et le Code de la santé publique sont ci-après ensemble désignés la «**Réglementation**»

Article 1 - Définitions

Annuaire : Ils permettent d'authentifier et identifier les **Utilisateurs** habilités. Ils permettent également aux **Utilisateurs** de retrouver des correspondants. **Medimail** repose aujourd'hui sur deux annuaires, l'annuaire **MSSanté** et l'annuaire **Medimail**.

ANS : Agence du Numérique en Santé

MSSanté : Espace de confiance qui regroupe les opérateurs de messageries électroniques réservé aux professionnels de santé. Il se caractérise par :

- L'annuaire national **MSSanté** des professionnels habilités à échanger des données de santé à caractère personnel et disposant d'une adresse de messagerie **MSSanté**
- Une liste blanche des domaines **MSSanté** regroupant les domaines des opérateurs détenteurs d'un certificat numérique d'authentification délivré par l'**ANS**.

Medimail : Messagerie Sécurisée de Santé opérée par **MiPih**, la messagerie est accessible soit par **Webmail** sur le site <https://medimail.mipih.fr>, soit en téléchargeant l'application **Medimail Mobile** sur les stores Android ou IOS.

Utilisateur : Utilisateur final de la solution, professionnel de santé, médico-social ou toute personne habilitée à utiliser et à traiter des données à caractère personnel et des données de santé.

Usager : Personne bénéficiant d'une prestation médicale ou médico-sociale dont les données font l'objet d'un traitement par la Messagerie Sécurisée de Santé.

Article 2 - Responsables de traitement

Dans le cadre de la protection des données à caractère personnel et des données de santé, le RGPD a en particulier introduit le rôle de **Responsable de traitement**, rôle repris dans la loi relative à l'informatique, aux fichiers et aux libertés (article 3 de la loi n°78-17 du 6 janvier 1978 modifiée). Il est défini comme suit par la CNIL " Le responsable d'un traitement de données à caractère personnel est, sauf désignation expresse par les dispositions législatives ou réglementaires relatives à ce traitement, la personne, l'autorité publique, le service ou l'organisme qui détermine ses finalités et ses moyens. En pratique et en général, il s'agit de la personne morale incarnée par son représentant légal.

- Chaque **Utilisateur** est responsable de traitement des données à caractère personnel relatives à l'**Usager** qu'il prend en charge.
- **MiPih** est responsable de traitement des données relatives aux **Utilisateurs** utilisant la messagerie **Medimail**.
- Le MiPih hébergeur certifié ISO 27001 et HDS est responsable de l'hébergement des données collectées par le biais de la messagerie **Medimail**.

En tant que **Responsable de traitement**, l'**Utilisateur** ou la structure qui l'emploie sont responsables de la délivrance d'informations aux **Usagers** sur l'utilisation d'une messagerie Sécurisée de Santé et doivent recueillir leur consentement.

L'**Usager** aura donc été informé et aura consenti au préalable à la collecte et au traitement de ses données de santé à caractère personnel par le biais d'une Messagerie Sécurisée de Santé et de l'hébergement de celles-ci chez un Hébergeur certifié HDS.

Les **Responsables de traitement** garantissent chacun pour ce qui les concerne que les données à caractère personnel de l'**Utilisateur** et de l'**Usager** ne seront transmises à aucun tiers non autorisé, sans leurs accords.

Article 3 - Données à caractère personnel collectées et conditions de conservation

3.1 Données de l'**Utilisateur**

Dans le cadre de leur inscription à la messagerie Sécurisée de Santé **Medimail** les professionnels de santé ou du secteur médico-social doivent fournir un certain nombre de données afin d'être identifiés comme **Utilisateurs** habilités à traiter les données à caractère personnel dont de santé des **Usagers**.

A ce titre, ils doivent fournir les données à caractère personnel suivantes :

- Nom – Prénom
- Adresse professionnelle (mail et adresse postale) - Numéro de téléphone
- RPPS ou ADELI
- Profession - Lieu exercice
- Données authentification.

A défaut de l'acceptation du traitement de ses données à caractère personnel, l'**Utilisateur** ne pourra pas souscrire au Service.

L'**Utilisateur** est informé que ses données à caractère personnel sont conservées dans les conditions suivantes :

- Pendant toute la durée de la relation contractuelle avec MiPih. Au-delà, les données sont conservées dans l'annuaire **MSSanté** sauf mention contraire.
- Par du personnel spécifiquement habilité, dans le strict respect de leurs missions uniquement à des fins de gestion technique des Comptes personnels
- Elles seront susceptibles de faire l'objet d'analyses et d'études statistiques, dans le respect de l'anonymat de l'**Utilisateur**, et après mise en œuvre de l'ensemble des formalités requises auprès de la CNIL lorsqu'elles sont applicables.
- Les messages sont conservés pour une durée de 3 mois, au-delà ils sont automatiquement supprimés.
- MiPih conserve les traces techniques et fonctionnelles pour une durée d'un an.

3.2 Données de l'**Usager**

Des données de santé à caractère personnel, recueillies à l'occasion d'activités de prévention, de diagnostic, de soins ou de suivi social et médico-social au sens de la **Règlementation**, sont susceptibles d'être collectées et traitées dans le cadre de l'envoi de messages, et à ce titre sont hébergées au **MiPih**, hébergeur certifié de données de santé.

Dans le respect des règles relatives au secret médical et au partage des données de santé couvertes par le secret médical, les informations concernant les **Patients** sont destinées exclusivement :

- Aux Professionnels de santé et Médico-sociaux sélectionnés par le **Patient** pour lui délivrer un Service
- Aux administrateurs strictement habilités de l'hébergeur certifié de données de santé, au sens de l'article L.1111-8 du Code de la santé publique, dans la limite de leurs attributions respectives
- Aux personnes habilitées au titre des tiers autorisés (les juridictions concernées, les arbitres, les médiateurs, les ministères concernés...)

L'**Usager** est informé que ses données à caractère personnel sont conservées dans les conditions suivantes :

- Les messages sont conservés pour une durée de 3 mois, au-delà ils sont automatiquement supprimés.
- Les messages sont hébergés au MiPih hébergeur certifié ISO 27001 et Hébergeur de Données de Santé

Article 4 - Droits des Utilisateurs et des Usagers

Conformément à la **Règlementation**, les **Utilisateurs** et les **Usagers** peuvent exercer leurs droits d'accès aux données qui les concernent et les faire rectifier ou les supprimer.

4.1 - Droit des **Utilisateurs**

Conformément à la Règlementation, l'**Utilisateur** est titulaire d'un droit d'accès, de rectification, d'opposition, de suppression des données à caractère personnel le concernant, qu'il peut exercer auprès du délégué à la protection des données (DPO) du **MiPih** spécifiquement habilité à répondre aux demandes des **Utilisateurs** identifiés qui pourront exercer leurs droits, par courrier électronique à l'adresse électronique suivante : dpo@mipih.fr ou par courrier au dpo du MiPih – 12 rue Michel Labrousse - 31100 Toulouse.

L'**Utilisateur** est également titulaire des droits suivants qu'il exerce suivant les mêmes modalités :

- un droit à l'effacement (droit à l'oubli) ;

- un droit d'opposition au regard du traitement des données à caractère personnel le concernant
- un droit d'introduire une réclamation auprès de la CNIL

L'**Utilisateur** reconnaît qu'il peut, à tout moment, retirer son consentement et s'opposer au traitement de ses données à caractère personnel en demandant la clôture de son Compte personnel suivant les mêmes modalités. Des données peuvent être conservées dans l'Annuaire MSSanté, l'**Utilisateur** pourra faire valoir ses droits auprès de l'**ANS**.

4.2 Droits des **Usagers**

Conformément à la Règlementation, l'**Usager** dispose d'un droit d'opposition à l'hébergement des données à caractère personnel le concernant par un hébergeur.

L'**Usager** est également titulaire d'un droit d'accès, de rectification, d'opposition, de suppression des données à caractère personnel le concernant.

Une fois identifié, il peut exercer ses droits auprès du **Responsable de traitement**, à savoir le professionnel de santé ou Médico-Social **Utilisateur** de la Messagerie Sécurisée de Santé Medimail ou la structure qui l'emploie.

L'**Usager** est également titulaire des droits suivants qu'il exerce suivant les mêmes modalités :

- un droit à l'effacement (droit à l'oubli) ;
- un droit d'opposition au regard du traitement des données à caractère personnel le concernant
- un droit d'introduire une réclamation auprès de la CNIL

Article 5 - Violation de données à caractère personnel

En cas de violation de données à caractère personnel, le **Responsable de traitement** ou son sous-traitant s'engage à notifier l'incident auprès de l'autorité de contrôle dans les délais impartis (dans les 72h après connaissance des faits) et de prévenir les personnes concernées si nécessaire.

Article 6 - Traitement d'une saisie ou de réquisition judiciaire des données

Dans le cadre d'une procédure juridique MiPih est tenu de répondre positivement à la requête après vérification de la validité de la demande (mandat).